## CLAIMS

1. (Currently Amended) A computer-readable storage media comprising computer-executable instructions that, when executed by a processor, perform steps ~~method~~ comprising:

receiving a manifest defining first, second, and third code assemblies that are members of at least one application, wherein the manifest defines at least one trusted application and application evidence for making a trust decision;

evaluating the application evidence to determine if the at least one application is trusted;

generating a first, a second, and a third permission grant set for the first, the second, and the third code assembl~~[[y]]~~ies, respectively, that are members of the at least one application if the application evidence satisfies at least one condition for trusting the at least one application;

passing the permission grant sets to a run-time call stack;

calling the second code assembly by the first code assembly;

calling the third code assembly by the second code assembly, the third code assembly attempting access of a protected file; and

calculating an intersection of the first and the second permission grant sets to determine whether the access to the protected file is permitted.

2. (Currently Amended) The ~~method~~ computer-readable storage media of claim 1 wherein the manifest further defines a plurality of code assemblies,

the method further comprising evaluating application evidence for a group of applications and generating a permission grant set for each code assembly that is a member of the group of applications if the application evidence satisfies at least one condition for trusting the group of applications.

3. (Currently Amended) The ~~method~~ computer-readable storage media of claim 1 wherein evaluating application evidence is based at least in part on an XrML license.

4. (Currently Amended) The ~~method~~ computer-readable storage media of claim 1 further comprising evaluating application evidence at an application level and a code assembly level before trusting the at least one application.

5. (Currently Amended) The ~~method~~ computer-readable storage media of claim 1 further comprising evaluating application evidence at a group level, an application level, and a code assembly level before trusting the at least one application.

6. (Cancelled)

7. (Cancelled)

8. (Currently Amended) The ~~method~~ computer-readable storage media of claim 1 further comprising determining if the first and second code assemblies are members of the at least one application.

9. (Cancelled)

10. (Currently Amended) The ~~method~~ computer-readable storage media of claim 1 wherein satisfying at least one trust condition is based at least in part on evidence provided with the at least one application.

11. (Currently Amended) The ~~method~~ computer-readable storage media of claim 1 wherein satisfying at least one trust condition is based at least in part on evidence external to the at least one application.

12. (Cancelled)

13. (Currently Amended) The ~~method~~ computer-readable storage media of claim 1 wherein satisfying at least one trust condition is based on evidence from user interaction.

14. (Currently Amended) The ~~method~~ computer-readable storage media of claim 1 wherein satisfying at least one trust condition is based on evidence from evaluation of previous trust decisions.

15. (Cancelled)

16. (Cancelled)

17. (Currently Amended) A ~~computer program product encoding a computer program for executing on a computer system a computer process, the computer process~~ computer-readable storage media comprising computer-executable instructions that, when executed by a processor, perform steps comprising:

receiving a manifest defining first, second, and third code assemblies that are members of at least one application, wherein the manifest defines at least one trusted application and application evidence for making a trust decision;

evaluating the application evidence to determine if the at least one application is trusted;

generating a first, a second, and a third permission grant set for the first, the second, and the third code assembly, respectively, that are members of the at least one application if the application evidence satisfies at least one condition for trusting the at least one application;

passing the permission grant to a run-time call stack;

calling the second code assembly by the first code assembly;

calling the third code assembly by the second code assembly, the third code assembly attempting access of a protected file; and

calculating an intersection of the first and the second permission grant sets to determine whether the access to the protected file is permitted, wherein both the first and the second permission grant sets need a permission to read the protected file such the third code assembly is permitted to access the protected file.

18. (Currently Amended) The ~~computer program product~~ computer-readable storage media of claim 17 wherein ~~the computer process further comprises~~ the manifest further ~~defining~~ defines a plurality of code assemblies and evaluating application evidence for a group of applications and generating a permission grant set for each code assembly that is a member of the group of applications if the application evidence satisfies at least one condition for trusting the group of applications.

19. (Currently Amended) The ~~computer program product~~ computer-readable storage media of claim 17 wherein the computer process further comprises evaluating application evidence based at least in part on an XrML license.

20. (Currently Amended) The ~~computer program product~~ computer-readable storage media of claim 17 ~~wherein the computer process~~ further

~~comprises~~ comprising evaluating application evidence at an application level and a code assembly level before trusting the at least one application.

21. (Currently Amended) The ~~computer program product~~ computer-readable storage media of claim 17 ~~wherein the computer process~~ further ~~comprises~~ comprising evaluating application evidence at a group level, an application level, and a code assembly level before trusting the at least one application.

22. (Cancelled)

23. (Cancelled)

24. (Currently Amended) The ~~computer program product~~ computer-readable storage media of claim 17 ~~wherein the computer process~~ further ~~comprises~~ comprising determining if the first and second code assemblies are members of the at least one application.

25. (Cancelled)

26. (Currently Amended) The ~~computer program product~~ computer-readable storage media of claim 17 wherein the ~~computer process is~~

computer-executable instructions are based at least in part on evidence provided with the at least one application.

27. (Currently Amended) The ~~computer program product~~ computer-readable storage media of claim 17 wherein the ~~computer process is~~ computer-executable instructions are based at least in part on evidence external to the at least one application.

28. (Cancelled)

29. (Currently Amended) The ~~computer program product~~ computer-readable storage media of claim 17 wherein the ~~computer process is~~ computer-executable instructions are based on evidence from user interaction.

30. (Currently Amended) The ~~computer program product~~ computer-readable storage media of claim 17 wherein the ~~computer process is~~ computer-executable instructions are based on evidence from evaluation of previous trust decisions.

31. (Cancelled)

32. (Cancelled)

33. (Currently Amended) A system comprising:

a processor;

a memory accessed by and operated on by the processor;

a manifest, configured as part of the memory, defining first, second, and third code assemblies that are members of at least one application, the first code assembly being a main code assembly, the second code assembly being a parser code assembly, and the third code assembly being a file access code assembly;

application evidence, stored in the memory, to determine whether the at least one application is trusted;

a loader, stored in the memory, to load the first, the second, and the third code assemblies into a run-time call stack, with the first code assembly calling the second code assembly, the second code assembly calling the third code assembly, with the third code assembly attempting access of a protected file; and

a policy manager, stored in the memory, to evaluate the application evidence relative to at least one condition, wherein the policy manager generates a first, second, and third permission grant set for the first, the second, and the third code assembly, respectively, that are members of the at least one application if the application evidence satisfies the at least one condition specified in a security policy specification for trusting the at least one application, wherein the security policy specification defines multiple policy levels, and wherein permissions are granted on a computer system based on the permission grant set, the policy manager further calculating an intersection of the first

and the second permission grant sets to determine whether the access to the protected file by the third code assembly is permitted, wherein both the first and the second permission grant sets need a permission to read the protected file such the third code assembly is permitted to access the protected file.

34. (Currently Amended) The system of claim 33 further comprising an XrML program authorization module, configured as part of the memory, operatively associated with the policy manager for evaluating application evidence including at least one XrML license.

35. (Original) The system of claim 33 wherein the policy manager evaluates evidence at a group level, an application level, and a code assembly level before the at least one application is executed.

36. (Cancelled)

37. (Previously Presented) The system of claim 33 wherein the policy manager further determines if the first and second code assemblies are members of the at least one application.

38. (Original)The system of claim 33 wherein the application evidence is provided with the at least one application.

39. (Original)The system of claim 33 wherein the application evidence is provided external to the at least one application.

40. (Original)The system of claim 33 wherein the application evidence includes at least an XrML license.

41. (Original)The system of claim 33 wherein the application evidence includes evidence provided via user interaction.

42. (Original)The system of claim 33 wherein the application evidence includes evidence from the evaluation of previous trust decisions.

43. (Original)The system of claim 33 further comprising a security policy specification defining at least one trust condition for an application component, wherein the policy manager evaluates the at least one trust condition in the security policy specification.

44-48. (Cancelled)